TERRI AGNEW: Bonjour et bonsoir. Bienvenue à cette séance du programme de renforcement de compétences d'At-Large de 2016 concernant les tendances actuelles en matière de sécurité qui ont un impact sur les titulaires de noms de domaine et sur les utilisateurs finaux, ce mercredi 19 octobre à 21 h 00 UTC.

Je voudrais vous rappeler, que vous soyez connecté à travers le téléphone ou à travers l'ordinateur, de mettre en lignes en muet, non seulement pour les procès-verbaux, mais également afin de permettre aux interprètes de vous identifier sur les canaux linguistiques. Nous avons des interprètes d'espagnol et de français.

Merci de nous avoir rejoints. Je donnerais maintenant la parole à Tijani Ben Jemaa, président du groupe de travail pour la formation de compétences.

TIJANI BEN JEMAA: Merci Terri. Nous voilà réunis pour ce séminaire web du programme de 2016 du groupe de travail de renforcement de compétences. Aujourd'hui, nous allons discuter des tendances de sécurité actuelles qui ont un impact sur les titulaires de noms de domaine et sur les utilisateurs finaux. Ce sujet a été sélectionné par notre spécialiste en sécurité, Julie Hammer, qui est également notre agent de liaison auprès de SSAC.

Je donnerais d'abord la parole au personnel qui fera quelques annonces administratives et par la suite, nous allons reprendre ce sujet.

TERRI AGNEW: Merci Tijani. J'aurais quelques annonces administratives à faire avant de commencer. Si vous voulez poser des questions au cours du séminaire web d'aujourd'hui, vous pouvez l'inscrire dans la caisse des questions-réponses qui est en bas à gauche dans la page d'Adobe Connect. Veuillez saisir votre question dans cette case pour qu'on la lise à la fin de la présentation. À la fin de la présentation, nous aurons également une question d'évaluation et j'espère que vous resterez jusqu'à la fin de l'appel pour faire l'évaluation de cet appel.

Donc, nous aurons les questions d'évaluation des connaissances et les questions d'évaluation administratives qui apparaitront en bas à droite.

Je voudrais également rappeler aux participants de compléter le sondage At-Large puisque que comme vous le savez, la communauté At-Large fait l'objet d'une révision en ce moment et je vous encourage à la compléter, à compléter cette enquête. Il s'agit d'un questionnaire qui est disponible en anglais, en français et en espagnol, qui rendrait à la communauté At-Large la possibilité de s'exprimer au sujet de questions d'importance pour elle.

Cela dit, je présente donc Julie qui va commencer.

JULIE HAMMER: Merci Terri. C'est un vrai plaisir d'avoir l'occasion de vous présenter Rod Rasmussen, qui est vice-président de sécurité dans sa société, et il est un expert reconnu dans le domaine du système des noms de domaine, surtout au niveau des attaques à la sécurité du système des noms de

domaine. Il a fondé une société qui se centre sur la réponse à l'incident, lié aux incidents de sécurité et au partage d'Informations.

Rod a également été une personne très active et a souvent occupé des rôles de direction dans l'industrie et dans les différentes organisations qui s'occupent des questions d'importance pour nous aujourd'hui. Rod participe également à différents groupes de travail sur les politiques et la sécurité d'Internet et sur les différentes questions d'importance en matière de sécurité. Les agents de liaison dans ce domaine… Il est membre du SSAC – un membre très actif d'ailleurs.

Rod appartient également au Comité de pilotage des alliances de travail de l'Internet et du Conseil d'incorruptibilité, de fiabilité et de résilience de l'Internet. Il travaille également avec les différents groupes de travail qui s'occupent de l'utilisation malveillante d'Internet et des cas d'abus et s'occupent du travail des équipes de réponse aux incidents et des équipes de sécurité qui représentent tant de différents utilisateurs internationaux.

Rod participe habituellement au comité de l'OARC, qui est l'Organisation mondiale d'opérateurs de registre et de fournisseurs de services. Voyez donc que Rod a toutes les connaissances nécessaires pour nous présenter ce sujet. C'est un plaisir pour moi de le présenter. Merci Rod.

ROD RASMUSSEN: Merci Julie et merci de participer à cet appel. J'espère pouvoir vous donner des informations au sujet des différentes questions d'aujourd'hui liées au DNS. Il s'agit d'un domaine que nous tenons tous

à cœur et qui nous intéresse beaucoup. Donc, sans plus, je vais commencer ma présentation. J'espère qu'elle sera claire.

Je voudrais que l'on se penche sur le DNS et sur les fins d'utilisation malveillante. Il serait possible de passer des heures à discuter de ces problèmes de cyber-sécurité et un grand nombre de ces questions sont discutées maintenant. Comme vous le savez, beaucoup de ce qu'on entend à la télé et beaucoup de ce qu'on entend dire implique le DNS dans l'équation des opérations. Vous savez que toutes nos opérations dépendent du DNS sur Internet, que ce soit pour envoyer un email, pour naviguer sur Internet ou pour d'autres types de communication que l'on souhaiterait établir à travers Internet. Mais tout dépend du DNS.

Lorsque l'on parle du DNS, si on demande où l'écosystème du DNS est atteint par ces utilisations malveillantes, on voit que cela se fait à travers les registres et à travers les bureaux d'enregistrement et bien sûr, à travers les différentes parties de l'Internet. Je partagerais également des idées pour pouvoir traiter ces problèmes, que ce soit au sein des différentes sociétés ou au sein des différents groupes de personnes intéressées par ce sujet. Et puis, des informations à considérer et des activités sur lesquelles nous travaillons au sein de l'ICANN. Voilà ma présentation que Julie vous a déjà faite.

Donc, je passerais maintenant directement au sujet de discussion. Je sais qu'on s'est déjà rencontré à certaines réunions de l'ICANN. D'habitude, on a des séances qui s'occupent des cas d'abus, des utilisations malveillantes lors des réunions publiques de l'ICANN, de la participation des communautés de registres et de bureaux d'enregistrement de ce qui se passe dans les différents domaines

d'intérêt. Il m'a semblé qu'il serait utile de prendre un peu de distance pour voir quel est l'impact de cela sur les organisations et sur les personnes ici. Donc, lorsqu'on parle de l'ICANN et de nos capacités, on sent qu'il y a beaucoup d'informations que les personnes qui s'occupent de ces questions connaissent déjà. Il y a des activités. On a différentes suppositions, différentes connaissances et différents faits que l'on prend pour acquis. Mais ce n'est pas toujours le cas.

Je voudrais donc aborder trois domaines différents d'intérêt. D'une part, on a les attaques qui portent atteinte à l'infrastructure du DNS elle-même. Il s'agit de l'utilisation du système contre les utilisateurs. Puis, on a l'utilisation du DNS en général pour des fins malveillantes : c'est l'utilisation de ces protocoles. Les bonnes personnes utilisent le DNS comme les mauvaises personnes. Donc, ces personnes qui veulent utiliser le DNS pour attaquer les personnes peuvent le faire tout simplement et c'est habituel de voir ce type d'utilisation malveillante sur Internet.

Finalement, nous allons parler de la manière d'envoyer des données qui ne sont pas les moyens prévus pour envoyer des données, mais qui sont utilisés par contre pour attaquer les victimes.

Parlons donc des cibles et des motivations, des raisons.

TERRI AGNEW: Pardon Rod. Je m'excuse de vous interrompre. Serait-il possible peut-être d'essayer de vous éloigner un peu du microphone ? Les interprètes n'arrivent pas à suivre exactement ce que vous dites. Vous n'êtes pas très clair.

ROD RASMUSSEN: C'est mieux ? Ça va mieux là ? Bien. Je vais parler des attaques du DNS et des services.

TERRI AGNEW: Non. Est-ce que vous pourriez vous éloigner un peu du micro peut-être ? C'est clair, mais c'est un peu trop faible. Je m'excuse.

ROD RASMUSSEN: Pardon. Est-ce que ça va mieux ?

TERRI AGNEW: Attendez. J'attends que les interprètes me confirment. Merci. Je vous remercie. Attendez.

TIJANI BEN JEMAA: C'est trop fort pour moi. Trop, trop fort.

TERRI AGNEW: Pardon Rod, mais malheureusement, ce n'est pas suffisant. Est-ce que vous avez un numéro de téléphone sur lequel on puisse vous contacter ?

ROD RASMUSSEN: Donnez-moi un instant.

TERRI AGNEW: Est-ce que vous voulez appeler vous-même ? Je n'ai pas compris ce que vous avez dit. C'est possible d'appeler vous-même si vous voulez.

ROD RASMUSSEN: Oui. Attendez. Je vais chercher le numéro de téléphone local de l'Australie. C'est bizarre, parce qu'elles m'entendaient très bien au début de l'appel. Maintenant, elles ne me comprennent pas. C'est malheureux.

TERRI AGNEW: Oui, Rod. Je vois sur le chat d'Adobe Connect…

ROD RASMUSSEN: Je vais vous donner le numéro de l'Australie. Oui, vous pouvez contacter les numéros de téléphone qui sont dans la case d'Adobe Connect.

TERRI AGNEW: Oui. Je m'excuse. On s'excuse, mais nous vous remercions de votre patience. Attendez. Non, ça ne fonctionne pas.

ROD RASMUSSEN: Je vais vous donner mon numéro pour que vous me contactiez.

TERRI AGNEW: Oui, je suis prête. L'opératrice va vous appeler dans quelques secondes.

ROD RASMUSSEN: Je suis connecté. Est-ce que ça va mieux ?

TERRI AGNEW: Oui. Attendez que je vérifie. Beaucoup mieux. On vous remercie. On s'excuse.

ROD RASMUSSEN: Oui. L'opératrice m'a dit que j'avais un petit problème aussi. On dirait que c'est un problème d'Adobe Connect. Je reprends donc ma présentation. L'idée ici portait sur les différentes attaques du DNS et les raisons pour lesquelles on faisait cela. Donc, voilà quelques attaques traditionnelles : pour cesser les services du serveur, on peut inonder par exemple le DNS ; pour avoir des opérations de corruption ; ou déconnecter l'infrastructure DNS. Donc, par exemple, on peut vous usurper l'identité, séquestrer le DNS, avoir des exploitations de vulnérabilité et des problèmes de reconnaissance.

C'est pour ça qu'on a mis en place le DNSSEC avec toutes les différentes informations. Donc, ces aspects de reconnaissance sont les mêmes. J'ai ici ajouté les informations sur le WHOIS et sur le DNS, puisque tout cela est lié en termes généraux à tous les gTLD, pour que toutes les personnes comprennent qui pourrait peut-être importer des attaques d'hameçonnage ciblées ou de mettre en place du pourriel, ou accéder à votre nom de domaine à travers le bureau d'enregistrement par exemple. Bien.

Voilà donc quelques informations des différentes attaques qu'il est possible d'intenter sur le DNS, contre le DNS, et qu'il est possible de gérer. Le DNS habilite la fourniture de services ou de contenus, même des services de connectivité tels qu'Adobe Connect par exemple. Donc,

lorsqu'on a par exemple des offres non souhaitées ou non voulues de services, il pourrait même y avoir des activités illégales : Les activités délictuelles par exemple pour voler de l'argent ou des données. Et bien sûr, certaines des activités malveillantes des acteurs de l'État pour contrôler les activités des utilisateurs sur Internet. Donc, tout cela est inclus dans cette gamme d'activités malveillantes, ennuyantes et même non souhaitées. Voyons maintenant certaines de ces techniques avec davantage de détails pour que ce soit plus clair.

Lorsque nous voyons les opérations à grande échelle des registres, comme par exemple l'enregistrement de noms de domaine qui n'est pas fiable. Dépendant de la juridiction, ce que l'on appelle fiable peut varier bien sûr. La définition de fiabilité varie, mais l'une des motivations principales de ce type d'enregistrement pour la mise en place de campagnes par email par exemple ou d'utilisation de différentes techniques pour pouvoir contourner les services qui dépendent de la fiabilité des services pour déterminer s'il s'agit d'une utilisation malveillante ou pas et qui pourrait filtrer des emails qui ne sont pas envoyés, parce qu'il semblerait qu'ils aient été envoyés par un nom de domaine qui n'est pas fiable, ou lorsque ce type de logiciels doive décider de vous permettre d'accéder à des sites ou pas pour le transfert d'informations également. Ces types de service utilisent la réputation des noms de domaine et les utilisent pour d'autres fins.

C'est pourquoi il faut mettre à jour périodiquement nos définitions du DNS et les sources de DNS. Et puis, on a d'autres aspects desquels dépendent les services du DNS. Donc, par exemple, il y a différentes structures qui ne respectent pas les lois locales dans le secteur pharmaceutique par exemple ou dans le domaine de la pornographie. Il

s'agit donc de branches qui utilisent des infrastructures et des fournisseurs non locaux pour ne pas être suspendu, qui utilisent des infrastructures d'ailleurs pour ne pas devoir respecter leur juridiction. Ils trouvent donc des juridictions auxquelles il n'y a pas ce type de lois et où ils ne feront pas l'objet de ce type de règlementations.

Nous travaillons sur ce problème depuis très longtemps et on essaye d'y trouver une solution. Il s'agit d'un problème qui est mitigé, mais qui n'est pas pour l'instant résolu et on travaille toujours avec les lois locales, avec les différentes ressources qui pourraient être disponibles dans les différentes juridictions. Donc, je pense que c'est un bon exemple de pourquoi les personnes enregistreraient leur nom de domaine et utiliseraient les ressources de noms de domaine dans d'autres juridictions que les leurs. On avance et on passe maintenant donc à l'utilisation de logiciels malveillants pour l'exploitation du DNS.

Les statistiques montrent que plus de 91 % des logiciels malveillants utilisent le DNS. Cela se fait pour obtenir le contrôle d'un canal. Donc, c'est comme si on utilise l'ordinateur de quelqu'un pour pouvoir saisir les ressources locales et leur dire quoi faire pour attaquer une autre personne ou pour éliminer des données d'un réseau, ou pour exfiltrer des données, pour rediriger le trafic par exemple et l'envoyer ailleurs.

Ce sont les types de mesure qui sont faites, tout ce qui contrôle et utilise le DNS pour pouvoir passer par les firewalls, par les pare-feux des ordinateurs. Tout cela est mitigé plus facilement par les adresses IP et ça nous permet donc de détourner l'utilisation des DNS et des ressources.

Cependant – et c'est ironique, à l'heure actuelle, il y a très peu d'organisations qui s'occupent de suivre les activités du DNS. Il y a de plus en plus de personnes qui le font, mais elles ne sont pas nombreuses pour l'instant. On a tous entendu parler de ce type d'utilisation malveillante, mais pourtant, on n'a pas suffisamment de mesures d'atténuation. Il est difficile de pouvoir informer de cela vu la quantité de noms de domaine enregistrés.

Surtout le meilleur exemple est la partie des logiciels de rançonnage qui augmentent de plus en plus. Un exemple ici est le nombre de délits, le niveau de délits au niveau du DNS. Le système de logiciels de rançon, c'est que je vais sur mon ordinateur après avoir vu qui vous étiez, je vais cliquer sur un lien ou sur une pièce jointe ou une adresse email et après avoir fait cela, je vais encrypter vos données et je vais refuser l'accès à votre adresse email. Je vais vous dire : « vous avez été piratés… pour avoir accès à vos données, normalement vous devez payer cette rançon en bitcoin ou en autre méthode difficile à situer. » Les délinquants en général demandent à être payé en bitcoin, parce que c'est plus difficile de remonter les données.

Donc, il faut apprendre à cibler et en général, ces attaques sont ciblées sur des petites ou moyennes entreprises, ou des avocats qui ont des données sensibles sur leur ordinateur et qui vont payer une rançon élevée. Cela est passé d'un problème de 50 millions de dollars jusqu'à beaucoup plus. On pense que les gens qui ont des données très sensibles qu'ils perdent sont capables de payer des sommes très élevées pour les récupérer.

Donc, c'est un phénomène très actuel : tout le monde devrait être prudent dans ce sens et il y a un grand manque de connaissances. 50 à 60 % des organisations ne sont pas au courant de ce problème et c'est donc un problème grave dont il faut tenir compte. Hélas, cela peut aller sur différents aspects et nous allons maintenant parler du système d'hameçonnage qui est encore très fréquent et qui évolue. On a ce système qui attaque des commerces. C'est une proportion assez élevée. Les effets sur les utilisateurs changent à l'origine. C'était que vous n'aviez pas d'habiletés, de possibilité de travailler dans votre juridiction. Tout dépend des services que vous utilisez et à ce moment-là, les activités criminelles vont changer. Il faut en tenir compte.

L'hameçonnage de notre site est un hameçonnage ciblé qui redevient une espèce de d'hameçonnage massif. Donc, il va avoir, va être plus largement ciblé et c'est quelque chose que l'on appelle… Ce sont des systèmes qui visent à s'approprier, à avoir accès à votre système d'emails et qui sont utilisés par un PDG ou un responsable important d'une compagnie pour utiliser son email, l'email de cette personne et prendre le contrôle des finances ou autre chose en disant : « Nous allons transférer 100 000 dollars à tel compte et nous allons utiliser ces informations ». À la base, c'est une escroquerie et cela arrive très souvent. Hélas, ce type d'actions a un impact au niveau commercial, peuvent provoquer des faillites graves dans des entreprises et il y a aussi les noms de domaine d'une organisation auxquels on envoie des emails de ce type de façon qu'on ait l'impression qu'il s'agisse d'une adresse correcte et cela risque de compromettre l'ensemble du nom de domaine. Donc, ce sont des faits, tout cela.

Voyons maintenant les statistiques pour la première partie de l'année 2016. Au niveau de l'hameçonnage, ce sont des données qui proviennent de l'APWG. Vous voyez que l'hameçonnage a augmenté ces derniers temps. On enregistre ici un nombre croissant de hameçonnages ces derniers mois. Quelles sont les cibles de ce hameçonnage pour les deux trimestres de l'année 2016 que nous avons ? Vous voyez sur le tableau ici, en bleu, les services de vente au détail, les services en général qui représentent presque un quart des cibles de ce hameçonnage. Ensuite, les services financiers et ce problème, le problème que le DNS est rarement contrôlé et en général, il est disponible. Donc, c'est un service léger qui permet, qui est sur le réseau et cela donne lieu à la capacité de tromper les gens et de tromper le DNS en transportant, en simulant des données, etc. Il y a un système que l'on appelle le tunneling, les attaques de tunnel du DNS que vous voyez ici. On va laisser des données exfiltrer en utilisant le DNS pour transmettre les données de cartes de crédit à des délinquants, ce qui pose de graves problèmes bien sûr. C'est un outil qui a été utilisé au niveau de l'espionnage et qui est train de devenir un outil qu'utilisent beaucoup les délinquants. Bien. C'est donc le type de délits qui existent au niveau du DNS.

Nous allons maintenant parler du secteur technique. C'est l'aspect technique lorsqu'on utilise la ressource du DNS, on utilise l'infrastructure du nom de domaine. Nous savons comment le faire. Cela est fait en utilisant une autorisation d'accès de paiement volé ou des comptes, des bitcoins par exemple. C'est gratuit. On voit ici la différence au niveau des activités quant au prix du domaine. Ces délinquants en général vont essayer d'obtenir tout cela gratuitement et

donc, ils demandent à être autorisés à rentrer sur ces réseaux et à utiliser un compte de bureau d'enregistrement compromis. Il y a des revendeurs aussi qui sont douteux, des personnes qui enregistrent des noms de domaine et toutes les autres choses.

Vous pouvez compromettre des sites Internet, vous pouvez aussi compromettre un opérateur DNS. C'est rare, mais cela arrive. Des personnes rentrent dans un serveur qui fournit des DNS. C'est, par exemple, parce que le mot de passe était faible ou il a été volé ou on utilise le même mot de passe à plusieurs endroits et pareil, compromettre un bureau d'enregistrement. On peut cambrioler un bureau d'enregistrement ou rentrer dans le compte d'un bureau d'enregistrement, parce qu'il utilise le même mot de passe ou bien simplement avoir accès à un ordinateur de ce bureau d'enregistrement. On voit rarement des attaques faites différemment dans les infrastructures des bureaux d'enregistrement. C'est rare. Voyons maintenant. Il y a un problème ici. On entend de la musique sur la ligne.

TERRI AGNEW: Ah. Nous nous excusons. Il y a un problème ici technique. Nous allons tenter de le résoudre.

ROD RASMUSSEN: Bien. Vous voyez ici sur ce graphique l'anatomie d'une attaque d'hameçonnage ciblé pour vous expliquer comment cela fonctionne et nous allons avancer rapidement, parce que comme ça je voudrais qu'on ait le temps pour les questions.

Donc, maintenant passons à cette diapo. Je vous parlais de techniques qui sont utilisées au sein du DNS et qui sont intéressantes, parce qu'elles sont uniques et elles vont vous montrer les possibilités. D'abord, il y a des années où nous avons eu une politique de fast flux ou flux rapide et des discussions ont eu lieu là-dessus. Des résolutions ont été prises. Il y a eu des politiques mises en œuvre. C'est un problème qui existe encore. On a un réseau d'ordinateurs mettons et je veux rediriger… Il y a des… C'est un flux qui va changer rapidement et l'utilisation du DNS et les enregistrements du DNS et qui va permettre de rester pendant un bon moment et de bloquer ou de fermer ce réseau. Je peux aussi modifier le nom, je peux aussi changer ou bloquer le nom du serveur, je peux aussi faire cela à plusieurs reprises.

Il y a différentes techniques et il y a des mécanismes de protection pour lutter contre cela. Donc, si l'on utilise la même technique qu'on peut utiliser au niveau local lorsqu'on a un nom de domaine, une direction, une adresse IP qui est plus proche. Ces adresses ont l'air d'être exactement les mêmes, mais il y a certaines petites différences entre elles qui sont presque invisibles. Ici, je crois que c'est l'anatomie d'une attaque de type fast flux que vous voyez ici. La personne va vouloir infecter des hôtes : elle va réunir cela dans un postnet. Cela va donner lieu en permanence à de nouvelles adresses, de nouvelles attaques et cela va être déclenché par des emails et peu importe… Cela va donner lieu à une infection de ma boite email. Ici, une formule pour les fast flux, les flux rapides. Il y a une série de manières de se protéger contre ce type de problèmes et on peut trouver tout cela si cela est nécessaire. Continuons à avancer.

Les algorithmes de génération de domaine. Il s'agit de ressources si j'ai une commande ou un contrôle d'un logiciel malveillant et si ce logiciel a été détecté depuis longtemps, on peut fermer le domaine ou travailler de différentes façons pour se protéger contre cela. Ce qui arrive aujourd'hui, c'est qu'on utilise un algorithme de génération de domaine qui va rentrer dans le logiciel malveillant et va donner une liste de domaines avec les jours de la semaine et les dates par exemple. Cela va… Le logiciel malveillant va essayer d'atteindre cette liste de domaines générés et va essayer de prendre le contrôle sur le serveur.

Cela va vous permettre d'être résilient dans le temps et de fournir des difficultés à ceux qui essayent de mettre en place ce système. Il y a toute une liste de ce type de logiciels malveillants qui change tous les jours. Donc si l'on contrôle le réseau, on peut voir ce type de choses, on peut les constater, parce qu'il y a une machine… On essaye d'atteindre un domaine qui n'existe pas et ce nom de domaine est étrange et n'existe pas. Donc, on peut trouver ce problème si on analyse. Les ingénieurs peuvent voir de quoi il s'agit ici.

L'histoire des DTA. En 2008, je sais que quelques-uns d'entre vous le connaissent, Kraken a été l'un des plus graves. On a essayé de fermer, d'arrêter la possibilité d'enregistrer ce type de choses. Il y avait 500 domaines par jour qui étaient attaqués et on a mis en place un groupe de travail pour essayer… Un groupe de registres et de titulaires qui ont essayé de bloquer ce système et il y avait… C'était vraiment un très gros problème à la fin de l'année 2008 donc.

Aujourd'hui, on a un standard, le Golden Standard, et on a des centaines et des centaines de différents DTA qui sont, qui existent. On

peut trouver… On a différents types de DTA qui existent. Donc, il a beaucoup de noms de domaine qui ont donné lieu à cela.

Il y a un grand nombre de documents partagés dans le domaine de l'industrie pour savoir de quoi il s'agit. On commence à avoir une certaine idée de ce type de problèmes. Ici, vous voyez à quoi ressemblent ces domaines.

Vous voyez ici qu'il n'y a pas de personnes enregistrées. Ce sont ce type de données encryptées et ce sont des techniques qui permettent de trouver ce type de choses et ce qui arrive ici, c'est qu'on va se dire : « C'est un problème. » On va essayer d'utiliser des dictionnaires, d'utiliser de véritables mots, des mots véritables et ça va nous donner un lien vers un dictionnaire, utiliser le dictionnaire.

Cela a été utilisé et ce qui arrive, c'est qu'avec ces logiciels malveillants, ils vont utiliser des mots et à chaque fois que vous les utilisez, on a donc ce type de listes. Très souvent, c'est très mauvais si vous avez, si vous êtes propriétaire d'un nom de domaine qui a été attaqué par ce type de DTA, parce que ce qui va arriver, tout va arriver dans votre système. Ils vont essayer de prendre le contrôle de votre système et vous allez ne plus avoir de service de nom de domaine pendant plusieurs jours.

Le résultat, c'est que vous aurez votre domaine qui sera dans une liste noire, ce qui peut être un problème. Donc, même si on connait ce type de logiciels malveillants, on ne sait pas comment résoudre ce type de problèmes. La meilleure manière de trouver ce DTA, c'est à travers des logiciels de détection du logiciel malveillant. Il y a différents types de logiciels et il est facile de trouver ce type de patron de motif.

Voilà des codes. C'est un peu trop technique. Je ne vais pas les lire. Je promets que je ne vais pas les lire. Je sais que c'est compliqué, mais bon, les machines savent le faire.

On a ici l'exfiltration de données. Bien. Il s'agit de la saisie de données à travers des requêtes de DNS. Donc, par exemple, si c'est une machine certifiée où des informations confidentielles devraient ne pas être dans le réseau, l'idée est de les éliminer sans que cela soit détecté. Si j'ai un logiciel malveillant, je pourrais dire : « Eh bien, je peux prendre ces données avec par exemple le nom de sécurité sociale, la date de naissance, peu importe ce que je veux. » Je ferais ces requêtes de DNS, je les enverrais et je dirais : « eh bien, mon idée est de les envoyer à une certaine adresse. » Le système va dire : « Je ne sais pas où c'est, je ne sais pas ce qu'est cette adresse. » La requête sera donc envoyée au serveur de noms : voleur.com par exemple. Moi, je demande Mary Smith voleur.com. Donc, à chaque fois que je demande, que j'envoie cette requête, cette même information va être envoyée.

Donc, à chaque fois qu'on envoie des requêtes de ce type, on va recevoir des réponses disant : «Ah, vous voulez les données de John Smith par exemple, je vous répondrais avec des informations de registre. » Donc par exemple, pour l'IP, il y aura des méthodes de verrouillage pour savoir ce qu'est ce type de requêtes. Le texte pourrait bien sûr être divisé en partie et envoyé à travers le DNS, utilisant également le registre TXP.

Donc, il faut vraiment faire attention au DNS pour pouvoir trouver ce type d'activités. Alors ici, cela a été fait par des services intelligents, des

États et voir quels sont les différents acteurs, mais surtout du secteur public.

Il existe une autre technique qui est le shadowing de domaine. C'est de demander à un service d'enregistrer un nom de domaine sous un nom de domaine qui existe vraiment. Donc, les personnes ou les criminels, par exemple, les délinquants utilisent ce type de méthode et ces services pour des propos malveillants. Ils utilisent donc une structure existante et ce qu'ils font pour ne pas être jugés qu'à la réputation du domaine, dont on parlait tout à l'heure, et d'utiliser des noms de domaines qui ont une bonne réputation. Mais ce qu'ils font, c'est transformer ce nom de domaine en site d'hameçonnage par exemple. Donc, ce qu'ils font est d'attaquer un bureau d'enregistrement qui fournit un service de DNS vers le panel de contrôle par exemple. Et par conséquent, il est facile pour eux de modifier cela. Ils ajoutent plein de noms de domaine hôtes, mais ne touchent pas le nom de domaine et le triple www. Donc, personne ne soupçonne ce qu'ils font, mais en même temps, ils utilisent d'autres registres à des fins délictueuses. Donc, les noms de domaine du registre, par exemple, sont utilisés pour ce type de but.

Donc, on voit des mesures, des contremesures, ce qui existe donc pour faire cela est un ensemble de logiciels d'exploitations qui envoient des informations aux ordinateurs victimes à travers leur navigateur par exemple et leur téléchargent des informations malveillantes. Donc, ils attaquent votre navigateur pour entrer dans votre ordinateur. Donc, par exemple, si on sait qu'un message fait partie d'une méthode d'hameçonnage, il faudra faire attention. Voilà, ce qu'est le shadowing

de domaine. C'est difficile parce qu'il est difficile d'analyser les ordinateurs pour trouver où se trouvent ces shadowing de domaine.

Donc, il faut vérifier tous les fichiers, tout ce qui est connecté pour les différents noms de domaine. Les réseaux par exemple sont utilisés pour envoyer ce type de publicité malveillante. Lorsque vous trouvez ces problèmes, si vous allez les résoudre, il faut notifier les différents comptes. Mais en matière d'intervention, on ne peut pas bloquer ce type d'activité. Pour les PME, les gens veulent pouvoir accéder à ce site web et c'est difficile. Il n'est pas facile de pouvoir décider s'il s'agit d'un shadowing de domaine ou pas. Voilà les problèmes. Nous allons maintenant passer aux mesures d'atténuation.

Ici, nous avons une liste des principales attaques, des principaux cas d'attaques du spam. Spamhaus a publié cette liste. Vous pouvez vous abonner à leur liste, donc Spamhaus. Ici, à travers cette liste, qui a été élaborée pour la communauté et qui est disponible sur leur site Web, identifie les dix principaux registres au niveau du TLD et les principaux bureaux d'enregistrement qui ont ce type de problèmes. Donc, dans le cas du .com par exemple, il y a beaucoup de problèmes. Donc, ce que Spamhaus a fait, c'est de créer une formule qui rationnalise suivant la taille des domaines existants et leur méthodologie, que je vous montrerais dans deux secondes, évalue les noms de domaines qu'il voit et qui sont envoyés dans différentes listes et qui sont partagés.

Par exemple, à travers des listes de courriels, ce qu'ils font c'est de voir la réputation du DNS dans les courriels qui sont envoyés et ajoutent des points d'observation aux différents serveurs de noms existants qui résolvent des noms. Donc, des fournisseurs de services Internet ou des

universités, lorsque vous voyez la réponse à la requête ou la taille de la requête : Qui c'est qui demande les informations, etc. ? Mais, il faut à chaque fois voir qui c'est qui demande et combien il demande, combien de fois il demande, quelle est la fréquence.

Donc, il identifie quelles sont les activités malveillantes, comment ces informations sont utilisées.

Ici, sur cette diapo, vous voyez où se trouvent ces problèmes pour quels noms de domaines surtout. Donc,= ici, vous avez les TLD et ce qui est intéressant sur ce tableur, c'est qu'il n'y a qu'un TLD hérité. Mais tout le reste, c'est des nouveaux gTLD. Ces numéros qui sont à l'écran montrent la superposition de ressources. Donc, vous voyez que certains nouveaux gTLD ont également des problèmes. Les nouveaux gTLD ont donc également des problèmes. Vous voyez .science, .top, par exemple, qui ont des fois plus de 300 000 cas de noms de domaine malveillants qui ont été enregistrés.

Et lorsqu'on évalue ces cas, par exemple, le .gdn est un nom de domaine générique qu'on a trouvé, parce qu'on se demandait où était tous ces sites d'exploitation du .gdn, et il s'agit de global domaine. C'est ça, « gdn » : global domaine names. Donc, ce tableur vous permet de voir ce qui se passe. Donc, on a ici les différents bureaux d'enregistrement qui ont des formules. On voit où le problème est observé dans la région impact. Donc, en Chine, au Japon, en Corée aussi surtout : il y a moniteur ici également. La quantité de TLD qui apparaît ici, qui sont indiqués, montre une tendance décroissante. Ici, nous avons les principaux bureaux d'enregistrement qui ont ce type de problèmes. [Inaudible] est celui qui a le plus de problèmes en ce

moment et nous voyons beaucoup de cas pour ce bureau d'enregistrement et on en discute beaucoup. On discute beaucoup de ce bureau d'enregistrement et de ces opérations et c'est bien sûr ce qui appartient au domaine de l'ICANN.

Donc, que fait l'ICANN ? Je sais qu'il y a certains bureaux d'enregistrement qui travaillent sur ce problème, qui essaient de le résoudre, mais le numéro 2 et le numéro 3 appartiennent à la même société. Ils sont relativement petits et ils appartiennent à la même société.

Ici, on a [Inaudible]. Il s'agit d'une autre société qui a une méthodologie différente et qui a un site Web où ce type d'informations est publié. Leur liste comprend tous les TLD.

Bien sûr, le .com est le nom de domaine, le TLD qui fait l'objet de plus d'abus bien sûr, mais ils évaluent plus de cent milliards de noms de domaine. Donc, vous voyez qu'en proportion, on n'a pas beaucoup de noms de domaine qui fassent l'objet de ce type d'abus. Donc, même sachant qu'il pourrait s'agir de TLD hérité – c'est le cas ici, on voit aussi beaucoup d'abus au niveau des nouveaux TLD. Il y a deux ccTLD sur la liste : .ru et .us aussi ; .ru a toujours eu beaucoup de problèmes. Il y a plus d'informations bien sûr sur les différents domaines, mais en tout cas, voilà les principaux.

Ces listes ont été mises à jour il y a quelques jours, mais en termes généraux, il faut savoir donc le principal qui est le fait qu'ils éliminent des sites lorsqu'ils ne font plus partie des TLD les plus utilisés. Donc, une fois qu'ils voient que la tendance diminue, ils mettent à jour cette liste.

Bien. Quelques remarques concernant [Inaudible] que je voulais discuter avec vous. Cette présentation bien sûr pourrait être améliorée et les programmes de TLD sont importants. Par exemple, dans le cas de .xyz, il y avait différentes informations, mais il s'agissait toujours des mêmes bureaux d'enregistrement.

.info et .org, par exemple, avaient des programmes agressifs, des programmes très actifs pour mitiger ce type de problèmes. Ces organisations avaient des programmes qui avaient été mis en place. Je ne sais pas s'ils étaient très effectifs, mais on avait travaillé sur la promotion du .org par exemple. Le .work, pardon, qui a disparu après l'augmentation du prix de .work, qui est passé de cinquante centimes à trois dollars quatre-vingt-dix-neuf. Comme ils ont augmenté le prix, la quantité d'enregistrement a diminué : c'est normal. Donc, il y a eu différentes actions de publicité qui ont été organisées, différents TLD qui utilisaient ce type de mesures et c'est imaginable. Mais bien sûr, ça a eu un impact sur leur chiffre d'affaires et ils ont essayé de résoudre ce problème.

Dans le cadre du .com, il est très rare de voir ce type de situation. Un nom de domaine en général coûte deux dollars par an, donc lorsque le prix augmente, c'est normal de voir cela.

Finalement, je voudrais vous présenter ici le sondage du hameçonnage mondial d'APWG. Certaines de ces données ont été remises au SSAC à Helsinki. Ce sont des données qui viennent également de l'association anti-hameçonnage chinoise APAC, qui rassemble toutes ces informations et qui n'ont qu'à être publiées.

L'idée est de discuter du hameçonnage ici, mais ces informations nous donnent une idée de ce qui se passe. Au niveau des statistiques qui apparaissent ici, on voit les différents rapports d'attaques. Et ce qui apparaît ici sont ceux qui ont été vérifiés. J'ai un tableur pour vous montrer ici l'historique de ces cas-là. Les TLD, par exemple, utilisés pour des activités d'hameçonnage sont pour la plupart des cas, à 75 %, utilisés à travers le compromis de la sécurité des TLD. Donc, si j'utilise mes ressources, les délinquants… Ce sont les délinquants qui utilisent ces ressources à des fins malveillantes.

Donc, on a vu beaucoup de shadowing de noms de domaine. On a vu l'ajout de nouveaux registres, on a vu des cas d'hameçonnage où les personnes malveillantes ont enregistré des noms de domaine. En 2010, par exemple, on voyait qu'il y avait beaucoup de problèmes, et des données, par exemple, concernant le prix qui avait augmenté ou qui pouvait diminuer pour des utilisations malveillantes, à des fins qui n'étaient pas correctes. Pour le cas de Google, c'était pareil et si vous voyez quel était l'opérateur dans ces domaines, il s'agissait du propriétaire du TLD qui fournissait la propriété à plusieurs personnes. Donc, il y avait plusieurs personnes qui s'étaient octroyé la propriété.

Vous voyez ici les statistiques. En 2016, elles ont un peu varié. Mais bien que la quantité d'abus ait, par exemple, diminuée dans certains cas, la quantité d'attaques a varié, mais les noms de domaines qui ont fait l'objet d'un hameçonnage ont augmenté.

Bien. Maintenant ici, vous voyez les résultats des attaques les plus élevés. Nous avons fait une classification de ces résultats de manière méthodique. Ici, dans ce cas-là, nous avons pris le nombre de domaines

avec les cas de hameçonnage divisés par le nombre de domaines où il y a vraiment eu ce type d'attaques et cela nous donne donc le résultat. Donc, c'est une estimation. La plupart des registres les publient eux-mêmes et vous voyez que le plus grand nombre d'attaques, ce sont des attaques individuelles.

Vous voyez qu'au niveau mondial, vous voyez ce type de pays. Les opérateurs de registres doivent savoir qui s'occupe, qui est situé sur les TLD. Donc, on a ici les rapports qui ont été faits. Il y a toute une série de rapports qui ont été faits à cause d'attaques individuelles. C'est quelque chose d'intéressant que nous avons fait et la façon dont on classe, la méthodologie qu'on utilise pour classer ce type de données nous permet de savoir vraiment ce qui se passe. Alors, regardons un petit peu maintenant les cas de noms de domaine qui ont été hameçonnés.

C'est différent du nombre d'attaques. Il peut y avoir des attaques faites sur le même nom de domaine. Ici donc, c'est les noms de domaines uniques utilisés pour le hameçonnage et les domaines qui ont souffert un hameçonnage pour un nombre de 10 000 domaines pour l'année 2015.

Ici, vous le voyez sur cette diapo et ce qu'on peut voir, c'est que le Venezuela est en général… Ce sont des ccTLD dans le cas du Venezuela. Et si on regarde un petit peu le contexte, il y a certains pays qui ont toujours été des problèmes et les gouvernements, les universités. Est-ce que ce type de choses en général… Ce sont des attaques qui sont des domaines qui ont été piratés avec .cfe, .gq, par exemple, .nl, qui ont fait des attaques de type marketing sur des ccTLD. Cela, on peut s'imaginer que ce genre de délinquants a accès à ces sites.

Et comme on a fait cette division, on a des chiffres très élevés. Par exemple, .cl, on a un chiffre élevé pour .cl. Il semble qu'il y a un problème ici, un problème de calcul. Ce chiffre n'est pas correct. Il ne correspond pas. En tout cas, le Venezuela et le Chili ont une place importante dans cette liste.

Ici, vous voyez les enregistrements malveillants. Ce sont des domaines qui ont été enregistrés par des délinquants et le Venezuela, de nouveau, est à une place importante dans le nombre d'enregistrements de domaine. Et c'est important parce qu'on voit que ces enregistrements peuvent avoir lieu ici : .cf, .gq, .ga, .ms, .cc, .pw. Tous ceux-là sont des domaines de type marketing, de style marketing.

Ensuite, .top, .party et .com, c'est intéressant parce que .com a 2,7 attaques. Donc, si on compare tout ce qui est en dessous de cela est trop grave et ça nous montre que le problème est concentré ici. Et la raison pour laquelle on utilise ce hameçonnage, je sais que c'est un système possible.

Bien. Observations pour l'enregistrement de domaine abusif. Les domaines qui ont un prix plutôt bas ou qui ne coûtent rien, ce sont les domaines qui souffrent le plus d'abus. Les ressources des délinquants sont aussi limitées et les changements dans les enregistrements abusifs suivent donc la promotion des prix de domaine pour les bureaux d'enregistrement et pour les titulaires de registre.

Certains revendeurs… Les recéleurs apparaissent et ensuite, un recéleur est interdit et ensuite, le même bureau d'enregistrement va avoir un autre revendeur. Donc, la plupart des nouveaux gTLD fonctionnent bien. On ne voit pas trop d'abus ou d'actions malveillantes.

Mais, on voit qu'il y a quand même des problèmes qui sont très concentrés et qui sont donc basés sur certains chiffres.

Alors, comment allons-nous conclure maintenant ? Nous allons vous donner quelques conseils pratiques pour vous protéger. Si vous avez votre nom, un propre, votre propre nom de domaine avec un bureau d'enregistrement et un fournisseur de DNS, n'utilisez pas le même mot de passe pour votre enregistrement. Si vous voulez éviter ce type de hameçonnage, refusez tout ce qui est le SPL et le DMA. Tout ce type de choses qui est disponible au niveau du bureau d'enregistrement ou des fournisseurs de noms de domaine. Si vous travaillez avec le DNSSEC, cela va vous aider aussi à résoudre ce type de problèmes.

Donc, utilisez le DNSSEC et utilisez la technologie et les services pour protéger, pour vous protéger de ces domaines donc abusifs. Au niveau de votre compagnie, vous devez faire attention parce qu'il y a certains… Il y a des logiciels malveillants qui deviennent de plus en plus courants et j'étais très sceptique auparavant par rapport à ces solutions anti-spam et je dirais que cela permet à l'utilisateur de se protéger.

Au niveau des individus, les filtres ou les bloqueurs d'ordinateur, les services de DNS propres, si vous pouvez l'utiliser pour nettoyer donc les services de DNS, pour s'assurer qu'il n'y ait pas de pourriel.

Si vous voulez utiliser ce type de système, ça va être utile et renseignez-vous avec le système donc de votre fournisseur Internet. Un anti-pourriel personnel bien sûr est utile et la campagne « Arrêtez, réfléchissez et connectez-vous », c'est important. C'est un message important. Faites attention, très souvent, avant de cliquer : il faut

réfléchir, parce que des fois certains liens si on clique dessus, on risque d'avoir de grosses difficultés.

Donc, APWG a mis en place cette campagne « Attendez, réfléchissez avant de vous connecter ». Je pense que c'est très important. Et quand on me pose une question ici, oui vous pouvez utiliser ces chiffres. Ces chiffres n'ont pas été publiés. Ce sont les dernières données que nous avons obtenues et je pense que vous pouvez les utiliser. Je ne sais pas quand est-ce que nous allons les publier, mais si vous voulez les utiliser, vous pouvez le faire. Allez-y.

Vous pouvez avoir accès aussi à cette présentation. Je vais vous la fournir et la dernière diapo. Donc, les questions politiques à considérer. Il y a une série de points ici, mais je dirais en général : Est-ce qu'on fait un bon travail pour le suivi, la mesure et le rapport des abus de manière pertinente ? Il y a des différences dans les méthodes, les catégories, les observations.

Comment est-ce qu'on décide de faire ce type de suivi, de surveillance et comment les mesurer ? Les décisions à prendre que cela entrainent et il faut donc recueillir des statistiques de manière pertinente et transparente. Pour trouver ces statistiques, il faut se rendre sur certains sites. Il n'y a pas eu beaucoup d'enregistrements sur ce type de données faits par des inventaires, faits comme ce que fait l'ICANN. L'ICANN ne fait pas ce type de choses par exemple.

On a un système de plaintes, mais on n'a pas un système pour enregistrer les abus. Alors, quels sont les mécanismes de protection que nous avons pour les titulaires de noms de domaine ? Il y a le SAC 40 et le SAC 44 qui ont été élaborés. Vu les problèmes que nous voyons, ils ne

sont pas ni en place, ni mis en œuvre par les bureaux d'enregistrement. Les bureaux d'enregistrement ont écouté certains conseils. Ils ont… Les délinquants ont des systèmes qui permettent de contrôler ces domaines, donc c'est un grave problème. Est-ce que nous avons ce type d'abus, ce type de problème à grande échelle ? Ce type d'enregistrement qui reste incorrect après de nombreux mois ou de nombreuses années, est-ce que nous avons pris des mesures appropriées pour lutter contre ces problèmes. Les gens dans le secteur de l'industrie apprennent les uns des autres à propos du type d'attaques qu'ils voient.

Donc, on met en place des méthodologies pour lutter contre le shadowing de domaine, par exemple. On va utiliser un système. On va aller voir un autre bureau d'enregistrement pour voir comment il travaille, partager des informations sur les délinquants avec eux et se protéger les uns les autres et la façon dont nous pouvons aussi fournir des manières plus efficaces d'enregistrer les abus.

Il faudrait mettre en place un système et je pense qu'au niveau des données et des commentaires qu'on peut recevoir de la part des gens qui luttent contre ce type de problème, il y a des rapports qui sont fait aux fournisseurs de services. Les fournisseurs de services réagissent par rapport à ces rapports et il serait bien de voir si on peut faire quelque chose pour encourager cette réponse-là de la part des fournisseurs de services pour trouver une meilleure manière de lutter contre ce problème. Voilà.

J'ai fini. Je vous remercie et c'était un peu long. Maintenant, je vous rends la parole.

TIJANI BEN JEMAA: Merci beaucoup, Rod, pour votre présentation. Je regrette, mais il ne nous reste plus que six minutes selon les horaires de notre cours en ligne. Alors, est-ce que vous avez des questions à poser à Rod ? Si c'est le cas, levez la main.

OLIVIER CRÉPIN-LEBLOND: J'ai levé la main.

TIJANI BEN JEMAA: Allez-y, Olivier. On n'avait pas vu.

OLIVIER CRÉPIN-LEBLOND: Merci Tijani. Oui. Donc, j'ai levé la main. Je vous remercie, Rod, pour cette présentation, ce séminaire Web. Je voudrais vous poser une question. Architelos faisait ce type de rapport aussi. Est-ce que vous avez utilisé les données qu'ils peuvent fournir aussi ? Je sais que vous participez ou je crois que vous participez au travail qu'ils réalisent aussi, non ? Au niveau de la lutte contre ce type de pourriel.

ROD RASMUSSEN: Greg est mon partenaire ici et dans ce travail, ma compagnie fournit les données à Architelos. Nous sommes une composante de leur travail, mais eux, le travail qu'ils obtiennent provient de différentes sources.

Le rapport qu'ils font, qu'ils ont fait, il y a certaines données qui venaient d'APWG, d'autres qui venaient de différentes organisations de volontaires. Ces volontaires travaillent avec nous depuis plus de dix ans

– comme volontaire, et on a un peu de mal ici à trouver d'autres volontaires. Mais je pense qu'on va pouvoir petit à petit améliorer notre travail, améliorer le système de recueil de données, de collecte de données et de suivi des compagnies aussi. Donc, toutes ces données, je les ai recueillies par ci par là pour mettre en place donc cette présentation.

TIJANI BEN JEMAA: Olivier, vous avez d'autres questions ?

OLIVIER CRÉPIN-LEBLOND: Oui, j'ai deux autres questions. Est-ce que je peux les poser ?

TIJANI BEN JEMAA: Oui, allez-y.

OLIVIER CRÉPIN-LEBLOND: La première est liée aux données que vous nous avez présentées dans cette présentation. Est-ce qu'on peut les utiliser ? Parce que lors des dernières réunions de l'ICANN, j'ai rencontré des gens dans les parties contractuelles et des gens du Conseil qui me disaient qu'il n'y avait pas de courriel grave, plus gravement, atteignant plus gravement les nouveaux gTLD. Et ici, d'après cette présentation, ce n'est pas le cas. Donc, il y a un problème par rapport à ces nouveaux gTLD.

Et ensuite, j'ai remarqué dans le chat qu'il y a eu une question de Ricardo Holmquist de l'ISOC du Venezuela. Et puisqu'ils sont assez mal qualifiés au Venezuela dans votre liste de pourriel, il demandait s'il

pouvait utiliser cette liste pour en parler avec donc les serveurs locaux, puisque ce problème les concernait pas mal.

ROD RASMUSSEN: Je réponds par oui à vos deux questions et j'ai répondu sur le chat aussi. Donc, allez-y. Utilisez mes diapos. Il n'y a pas de problème. APWG, tout le monde et tous ceux qui ont accès à ces documents connaissent ces chiffres. Donc, allez-y. Utilisez les. Il n'y a pas de problème. Voilà. Tout cela a déjà été publié. Donc, toutes ces données peuvent être utilisées et ont déjà été publiées. Voilà.

TIJANI BEN JEMAA: Merci. Il n'y a plus d'autres questions. Je demanderais à Terri de poser les questions.

TERRI AGNEW: Merci Tijani. Nous avons deux questions d'évaluation de connaissances pour voir si vous avez fait attention.

Question numéro 1 : Qu'est-ce que le shadowing de noms de domaine ? Veuillez voter maintenant.

Encore une fois, les questions apparaissent sur la droite.

Et Rod, une fois que tout le monde a voté, je vais vous demander quelle est la réponse correcte.

ROD RASMUSSEN: On a l'option numéro B qui est la correcte. C'est compromettre un nom de domaine en ajoutant des noms d'autres domaines et un faux DNS pour tromper les systèmes de réputation.

TERRI AGNEW: Merci. Question numéro 2 : les données montrent que les abus de noms de domaine tendent à corréler un bas prix pour les noms de domaine avec quelques exceptions. Est-ce vrai ou faux ? Veuillez voter maintenant.

Et Rod, veuillez, s'il vous plait, partager la réponse avec nous.

ROD RASMUSSEN: La réponse correcte est vraie. La liste de données que nous avions pour cette présentation ne fournit pas toutes ces réponses. Mais c'est le cas, c'est vrai.

TERRI AGNEW: Merci. Tijani, est-ce que vous voulez commenter ce que nous avons demandé ou on passe aux questions administratives ?

TIJANI BEN JEMAA: Non. Allez-y.

TERRI AGNEW: Très bien. Merci. Donc, nous allons maintenant poser quelques questions concernant l'administration de ce séminaire. Veuillez s'il vous plait rester quelques minutes de plus pour répondre à ces questions.

Question numéro 1 : Que pensez-vous de l'heure du webinaire pour vous ? Veuillez voter maintenant.

Question numéro 2 : Vous habitez dans quelle région en ce moment ? Veuillez voter maintenant.

Question numéro 3 : Combien d'années d'expérience avez-vous au sein de la communauté de l'ICANN ? Veuillez voter maintenant.

Question numéro 4 : Que pensez-vous de la technologie utilisée pour le séminaire web au niveau de l'audio, de la connexion téléphonique ?

Question numéro 5 : Est-ce que le présentateur maitrisait le sujet ?

Deux autres questions et nous vous remercions de votre temps. Etes-vous satisfaits du séminaire web ? Et question finale qui restera à l'écran. Veuillez prendre votre temps pour répondre. Quels sujets aimeriez-vous couvrir pour les séminaires à venir ?

Encore une fois, je vous remercie tous d'avoir participé à ce séminaire d'aujourd'hui. Rappelez-vous s'il vous plait de déconnecter vos lignes et ayez une bonne fin de journée.

JULIE HAMMER: Merci Terri. Avant de nous déconnecter, je voudrais remercier Rod qui a préparé et présenté ce séminaire web et le remercier au nom de nous tous. Nous lui sommes très reconnaissants. Merci Rod.

TIJANI BEN JEMAA: Merci Terri. Merci Rod. Merci Julie. Merci au personnel, aux interprètes. Merci à tous. Au revoir.

TERRI AGNEW: Merci à tous. Encore une fois, la réunion est maintenant finie. Merci de nous avoir rejoints et rappelez-vous, s'il vous plait, de déconnecter vos lignes. Ayez une bonne fin de journée.

[FIN DE LA TRANSCRIPTION]